ELSEVIER

Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®

Journal of Pure and Applied Algebra 188 (2004) 45–57

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Hopf–Galois structures on Galois field extensions of degree pq

Nigel P. Byott

Department of Mathematical Sciences, University of Exeter, Exeter EX4 4QE, United Kingdom

Received 15 July 2003; received in revised form 28 August 2003
Communicated by C. Kassel

Abstract

We determine all Hopf–Galois structures on a Galois extension of fields of degree pq, where p, q are primes with $p \equiv 1 \pmod{q}$. There are $2q-1$, respectively $2+p(2q-3)$, Hopf–Galois structures when the extension is cyclic, respectively nonabelian. Explicit generators are given for the groups of permutations corresponding to these Hopf–Galois structures.

MSC: 12F10; 16W30

1. Introduction

If L/K is a finite Galois extension of fields with group G then by the Normal Basis Theorem, L is a free rank 1 module over the group algebra $K[G]$. The fact that G acts on L as field automorphisms can be expressed in terms of the Hopf algebra structure of $H = K[G]$ by saying that L is an H-Galois extension of K. More generally, a Hopf–Galois structure on an arbitrary field extension L/K consists of a K-Hopf algebra H and an action of H on L making L into an H-Galois extension. For a finite separable field extension L/K, Greither and Pareigis [7] have shown how to recast the problem of finding all Hopf–Galois structures on L/K as a question in group theory which can be completely answered in some cases. If L/K is in fact a Galois extension with group G, then L/K certainly admits the classical Hopf–Galois structure with $H = K[G]$, but

E-mail address: n.p.byott@exeter.ac.uk (N.P. Byott).

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2003.10.010

there may in addition be a number of other (nonclassical) Hopf–Galois structures. In particular, there is always at least one nonclassical Hopf–Galois structure if G is not abelian, but there is only the classical Hopf–Galois structure if the degree n of L/K satisfies $\gcd(n, \varphi(n)) = 1$ where φ is the Euler totient function [1]. (This condition forces G to be cyclic.) As a consequence of the work of Kohl [8] it is known that, for an odd prime p, there are p^{m-1} Hopf–Galois structures on a cyclic extension of degree p^m. Carnahan and Childs [3] have shown that when G is the symmetric group S_n (with $n \geqslant 5$), there are at least $(n!)^{1/2}$ Hopf–Galois structures. Childs [6] has recently obtained results for the case where G is the holomorph of a cyclic group of odd prime-power order p^e, showing in particular that there are precisely $2 + 5p + 4pq$ Hopf–Galois structures if $e = 1$ and $q = (p-1)/2$ is also an odd prime. On the other hand, if G is a nonabelian simple group, then there are only two Hopf–Galois structures [2]. A detailed exposition of this theory up to 2000 can be found in [5].

As explained below, the Hopf–Galois structures on L/K correspond to certain subgroups N of the group $\mathrm{Perm}(G)$ of permutations of G. These subgroups will have the same order as G, but need not be isomorphic to G. Using an observation of Childs [4], one can find them by considering in turn each isomorphism type of group N of order $|G|$. (This can be avoided in the special cases considered in [8,2]). It therefore makes sense to investigate simultaneously the Hopf–Galois structures on all Galois extensions L/K of a given degree n, at least in cases where the number of isomorphism types of group of order n is small. This approach was adopted in [1] to show that for any prime p there are p (respectively, p^2) Hopf–Galois structures on a cyclic (respectively, elementary abelian) extension of degree p^2. In this paper, we carry out the same procedure for groups of order pq, where p and q are primes with $p \equiv 1 \pmod{q}$. There are then two isomorphism classes of groups to consider. We shall determine the number of Hopf–Galois structures, and give explicit generators for the corresponding subgroups N of $\mathrm{Perm}(G)$. The case $p \not\equiv 1 \pmod{q}$ is excluded since in this case any Galois extension of degree pq is cyclic and, by Byott [1], admits only the classical Hopf–Galois structure.

We intend to give a similar treatment for Galois extensions of degree p^2q and of degree p^3 in future papers.

2. Preliminaries

We consider only the situation where L/K is a finite Galois extension with group G. The more general case where L/K is separable but not necessarily normal is considered in [7]. In our setting, the main result of Greither and Pareigis [7] states that the Hopf–Galois structures on L/K correspond bijectively to regular subgroups N of $\mathrm{Perm}(G)$ normalised by G. Here G is viewed as embedded in $\mathrm{Perm}(G)$ as left translations. A subgroup N of $\mathrm{Perm}(G)$ is said to be regular if its action on G is transitive and the stabiliser of any point is trivial. In the Hopf–Galois structure corresponding to N, the Hopf algebra acting on L is $H = L[N]^G$, the fixed points of the group algebra $L[N]$ under the action of G simultaneously on L as field automorphisms and on N by conjugation inside $\mathrm{Perm}(G)$. For a given Hopf–Galois structure on L/K, we will refer

to the isomorphism class of the corresponding group N as the *type* of the Hopf–Galois structure.

Childs [4] showed that one may reverse the relationship between G and N: if N is as above then G embeds as a regular subgroup of the holomorph $\mathrm{Hol}(N)$ of N, where we view $\mathrm{Hol}(N)$ as a subgroup of $\mathrm{Perm}(N)$. However, the embedding of G into $\mathrm{Hol}(N)$ (respectively, of N into $\mathrm{Perm}(G)$) may be composed with an automorphism of G (respectively, N) without changing its image. Thus (see [1]) the number $e(G,N)$ of Hopf–Galois structures on L/K of type N can be calculated from the formula

$$e(G,N) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e'(G,N), \tag{2.1}$$

where $e'(G,N)$ is the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G. This provides our basic strategy for counting Hopf–Galois structures on Galois field extensions of degree n. We consider in turn each group N of order n. We determine the regular subgroups G in $\mathrm{Hol}(N)$ (together with their isomorphism types) and hence calculate $e'(G,N)$ for each isomorphism type G. When this has been done for all N, we consider each isomorphism type G in turn: the number of Hopf–Galois structures on a field extension with group G is $\sum_N e(G,N)$, where the sum is over all isomorphism types of group N of order n, and the summands $e(G,N)$ are given by (2.1).

Recall that $\mathrm{Hol}(N)$ is the semidirect product of N by $\mathrm{Aut}(N)$:

$$\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) = \{\eta\alpha : \eta \in N, \alpha \in \mathrm{Aut}(N)\}.$$

For typographical convenience, we use the exponential notation $\eta^\alpha = \alpha(\eta)$, even though we view $\mathrm{Aut}(N)$ and $\mathrm{Hol}(N)$ as acting from the left. The relation $\alpha\eta = \eta^\alpha\alpha$ in $\mathrm{Hol}(N)$ implies that

$$(\eta\alpha)^k = \eta^{1+\alpha+\alpha^2+\cdots+\alpha^{k-1}}\alpha^k$$

for all $k \geqslant 0$.

If G is a regular subgroup of $\mathrm{Hol}(N)$ then, projecting to $\mathrm{Aut}(N)$ and N, we obtain respectively a homomorphism $\Theta : G \to \mathrm{Aut}(N)$ and a bijection $\Phi : G \to N$ satisfying the cocycle relation $\Phi(gg') = \Phi(g)\Phi(g')^{\Theta(g)}$. We have $\Phi(g) = g \cdot 1_N$. The action of N on G corresponds under Φ to the left regular action of N on itself. Thus we can recover the action of N on G by defining

$$n \cdot g = \Phi^{-1}(n\Phi(g)) \in G \quad \text{for all } n \in N,\ g \in G. \tag{2.2}$$

The groups G_l, G_r of left (respectively, right) translations by N are among the regular subgroups of $\mathrm{Hol}(N)$. These are then among the possibilities for G which are isomorphic to N. We have $G_l = G_r$ precisely when N is abelian. Under (2.2), G_l (respectively, G_r) corresponds to the action of N on G by left (respectively, right) translations, and in this case Φ is an isomorphism (respectively, anti-isomorphism) of groups. It is the action of N on G by right translations which gives the classical Hopf–Galois structure.

It is convenient to enumerate the regular subgroups G of $\mathrm{Hol}(N)$ according to the size of their image $\Theta(G)$ in $\mathrm{Aut}(N)$. For each divisor m of $|G|$ we therefore define $e'(G,N,m)$ to be the number of regular subgroups of $\mathrm{Hol}(N)$ isomorphic to G whose

image in $\mathrm{Aut}(N)$ has order m, and set

$$e(G,N,m) = \frac{|\mathrm{Aut}(G)|}{|\mathrm{Aut}(N)|} e'(G,N,m). \tag{2.3}$$

When $m = 1$ the only candidate for such a subgroup is (left translations by) N itself, so

$$e(N,N,1) = 1, \quad e(G,N,1) = 0 \text{ if } G \text{ and } N \text{ are not isomorphic.} \tag{2.4}$$

The number of Hopf–Galois structures of type N on a Galois extension with group G is then given by $\sum_m e(G,N,m)$, where the sum is over all divisors m of $|G|$.

3. The groups of order *pq*

For the rest of the paper, we fix two primes p, q with $p \equiv 1 \pmod{q}$. Once and for all we fix an integer $g > 1$ whose order modulo p is q. For later use, we set

$$s(r) = \sum_{i=0}^{r-1} g^i = (g^r - 1)/(g - 1) \tag{3.1}$$

and, more generally,

$$s(r,d) = \sum_{i=0}^{r-1} g^{di} = (g^{dr} - 1)/(g^d - 1) \quad \text{for } r, d \geqslant 0. \tag{3.2}$$

Also, let a_0 satisfy

$$(g - 1)a_0 \equiv 1 \pmod{p}. \tag{3.3}$$

For arbitrary m, we write C_m for the cyclic group of order m.

Up to isomorphism, there are two groups N of order pq to consider:

3.1. The cyclic group C

It is convenient to work with the presentation

$$C = C_{pq} = \langle \sigma, \tau \mid \sigma^p = \tau^q = 1, \tau\sigma = \sigma\tau \rangle. \tag{3.4}$$

As $\mathrm{Aut}(C) = C_{p-1} \times C_{q-1}$, any homomorphic image in $\mathrm{Aut}(C)$ of a group of order pq must lie in the subgroup of C_{p-1} of order q. Thus any regular subgroup of $\mathrm{Hol}(C)$ lies in $N \rtimes A(C)$ where $A(C) = \langle \alpha \rangle \cong C_q$, with the action of α on C given by

$$\sigma^\alpha = \sigma^g, \quad \tau^\alpha = \tau. \tag{3.5}$$

3.2. The metacyclic group M

This has presentation

$$M = \langle \sigma, \tau \mid \sigma^p = \tau^q = 1, \tau\sigma = \sigma^g\tau \rangle. \tag{3.6}$$

In the notation of (3.1) we have

$$(\sigma^c\tau)^r = \sigma^{cs(r)}\tau^r$$

for any integer c. Any automorphism ϕ of M must induce an automorphism of the characteristic subgroup C_p, so $\sigma^\phi = \sigma^a$ and $\tau^\phi = \sigma^b\tau^c$ with $1 \leqslant a \leqslant p-1$, $0 \leqslant b \leqslant p-1$ and $1 \leqslant c \leqslant q-1$. For ϕ to be compatible with the relation $\tau\sigma = \sigma^g\tau$ we require $c = 1$. Thus $\mathrm{Aut}(M)$ is a metabelian group of order $p(p-1)$, and any homomorphic image of a group of order pq in $\mathrm{Aut}(M)$ must lie in the group $A(M) = \langle\alpha, \beta\rangle$, where

$$\sigma^\alpha = \sigma, \quad \tau^\alpha = \sigma\tau; \quad \sigma^\beta = \sigma^g, \quad \tau^\beta = \tau. \tag{3.7}$$

We then have $\alpha^p = 1 = \beta^q$ and $\beta\alpha = \alpha^g\beta$, so $A(M) \cong M$.

4. Regular subgroups in Hol(C)

Since $A(C) = C_q$, we need to determine $e(G, C, m)$ for $m = 1$ and q, and for $G = C$ and M.

4.1. $m = 1$

From (2.4) we have

$$e(C, C, 1) = 1, \quad e(M, C, 1) = 0. \tag{4.1}$$

4.2. $m = q$

Lemma 4.1. *We have*

$$e(M, C, q) = p, \quad e(C, C, q) = 0. \tag{4.2}$$

The p subgroups of $\mathrm{Perm}(M)$ *giving the Hopf–Galois structures counted by $e(M, C, q)$ are the groups N_c for $0 \leqslant c \leqslant p-1$, where N_c is generated by the two permutations*

$$\sigma^u\tau^v \mapsto \sigma^{u+1}\tau^v, \quad \sigma^u\tau^v \mapsto \sigma^{u-cg^v}\tau^{v+1}. \tag{4.3}$$

Here $\sigma^u\tau^v$ denotes an arbitrary element of M.

Proof. If G is a regular subgroup of $\mathrm{Hol}(C)$ with image C_q in $\mathrm{Aut}(C)$ then $G \cap C = \langle\sigma\rangle$, so

$$G = \langle\sigma, \tau^b\alpha\rangle \tag{4.4}$$

for some b, where α is given by (3.5) and σ, τ are as in (3.4). We calculate $(\tau^b\alpha)^q = \tau^{bq}\alpha^q = 1$ and $(\tau^b\alpha)\sigma = \tau^b\sigma^g\alpha = \sigma^g(\tau^b\alpha)$. Thus for any choice of b, the above group G is indeed of order pq and $G \cong M$. Now $(\tau^b\alpha)^k \cdot 1_N = \tau^{bk}\alpha^k(1_N) = \tau^{bk}$ for any k, so G is regular if and only if $b \not\equiv 0 \pmod q$. We obtain $q-1$ different groups G by taking $1 \leqslant b \leqslant q-1$. Hence $e'(M, C, q) = q-1$ and $e'(C, C, q) = 0$. Using (2.3), we then obtain (4.2).

To determine explicitly the subgroups $N \cong C$ of $\mathrm{Perm}(M)$ counted by $e(M,C,q)$, we apply (2.2). We first write $\sigma_G = \sigma$, $\tau_G = \tau^b\alpha$ for the generators of $G \subset \mathrm{Hol}(C)$ in (4.4). These satisfy the same commutation relation as in (3.6), allowing us to identify G with M. For arbitrary $g = \sigma_G^u\tau_G^v \in G$ we have $\Phi(g) = \sigma^u\tau^{bv}$. Thus

$$\sigma \cdot g = \Phi^{-1}(\sigma^{u+1}\tau^{bv}) = \sigma_G^{u+1}\tau_G^v$$

and

$$\tau^b \cdot g = \Phi^{-1}(\tau^b\sigma^u\tau^{bv}) = \sigma_G^u\tau_G^{v+1}.$$

We therefore obtain the subgroup of $\mathrm{Perm}(G)$ generated by left translation by σ_G and right translation by τ_G. As this is independent of b, we have so far found only one of the p subgroups N we are seeking. Equivalently (up to composing with an automorphism of C), we have found one of the possible embeddings of C into $\mathrm{Perm}(M)$. To obtain the others, we conjugate N by automorphisms of G, which corresponds to composing the embedding with automorphisms of M. Let $\gamma = \alpha^c$ for $0 \leqslant c \leqslant p-1$, where now $\alpha \in \mathrm{Aut}(G)$ is given in (3.7). Then $(\sigma_G^u\tau_G^v)^\gamma = \sigma_G^u(\sigma_G^c\tau_G)^v = \sigma_G^{u+cs(v)}\tau_G^v$, so

$$\sigma \cdot (\sigma_G^u\tau_G^v)^\gamma = (\sigma_G^{u+1}\tau_G^v)^\gamma$$

and

$$\tau^b \cdot (\sigma_G^u\tau_G^v)^\gamma = \sigma_G^{u+cs(v)}\tau_G^{v+1} = (\sigma_G^{u-cg^v}\tau_G^{v+1})^\gamma.$$

Dropping the subscripts G, we obtain the subgroups N_c of $\mathrm{Perm}(M)$ defined in the statement of the lemma. □

5. Regular subgroups in Hol(M)

Since $A(M) \cong M$, we need to determine $e(G,M,m)$ for $m = 1$, p, q and pq, and for $G = C$ and M.

5.1. $m = 1$

From (2.4) we have

$$e(M,M,1) = 1, \quad e(C,M,1) = 0. \tag{5.1}$$

5.2. $m = p$

Lemma 5.1. *We have*

$$e(C,M,p) = q-1, \quad e(M,M,p) = 0. \tag{5.2}$$

The $q-1$ subgroups of $\mathrm{Perm}(C)$ *giving rise to the Hopf–Galois structures counted by $e(C,M,p)$ are the groups N_d for $1 \leqslant d \leqslant q-1$, where $N_d \cong M$ is generated by the two permutations*

$$\sigma^u\tau^v \mapsto \sigma^{u+g^{-dv}}\tau^v, \quad \sigma^u\tau^v \mapsto \sigma^u\tau^{v+1}. \tag{5.3}$$

Here $\sigma^u\tau^v$ denotes an arbitrary element of C, and g^{-dv} is to be interpreted mod p.

Proof. Let G be a regular subgroup of $\mathrm{Hol}(M)$ with image of order p in $\mathrm{Aut}(M)$. Then this image is generated by the automorphism α of M defined in (3.7), and $G\cap M$ is a subgroup of M of order q. Thus $G\cap M=\langle\sigma^c\tau\rangle$ with $0\leqslant c\leqslant p-1$. Here σ and τ are as in (3.6). Multiplying a preimage of α in G by a suitable power of $\sigma^c\tau$, we see that

$$G=\langle\sigma^a\alpha,\sigma^c\tau\rangle \tag{5.4}$$

for some a, c. For such a group to have order pq, we require the subgroup $\langle\sigma^a\alpha\rangle$ to be normalised by $\sigma^c\tau$, so that, for some f with $1\leqslant f\leqslant p-1$, we have

$$(\sigma^c\tau)(\sigma^a\alpha)=(\sigma^a\alpha)^f(\sigma^c\tau),$$

that is,

$$\sigma^{c+ag}\tau\alpha=\sigma^{af+c+f}\tau^f\alpha^f.$$

This forces $f=1$, so that G is cyclic, and also $a=a_0$, where a_0 is defined in (3.3). We therefore have p possible groups G in (5.4), all of which are cyclic and are regular on M. Thus $e'(C,M,p)=p$ and $e'(M,M,p)=0$. Using (2.3), we then have (5.2).

To identify the $q-1$ subgroups N of $\mathrm{Perm}(C)$ counted by $e(C,M,p)$, we may take $c=0$ in (5.4) since the other values of c will be obtained by conjugating the action by an automorphism of M. Let $\sigma_G=\sigma^{a_0}\alpha$, $\tau_G=\tau$ be the generators of $G\cong C$ in (5.4). For an arbitrary element $g=\sigma_G^u\tau_G^v=\tau_G^v\sigma_G^u$ of G we have

$$\Phi(g)=\Phi(\tau^v\sigma^{a_0u}\alpha^u)=\tau^v\sigma^{a_0u},$$

so by (2.2),

$$\tau\cdot g=\Phi^{-1}(\tau^{v+1}\sigma^{a_0u})=\tau_G^{v+1}\sigma_G^u$$

and

$$\sigma^{a_0}\cdot g=\Phi^{-1}(\sigma^{a_0}\tau^v\sigma^{a_0u})=\Phi^{-1}(\tau^v\sigma^{a_0(g^{-v}+u)})=\tau_G^v\sigma_G^{g^{-v}+u}.$$

These give the permutations generating one of the required subgroups N of $\mathrm{Perm}(C)$. To find all of these subgroups, we conjugate by the automorphisms γ of C with

$$\sigma_G^\gamma=\sigma_G,\quad \tau_G^\gamma=\tau_G^d, \tag{5.5}$$

where $1\leqslant d\leqslant q-1$. Now

$$\sigma^{a_0}\cdot(\tau_G^v\sigma_G^u)^\gamma=\tau_G^{dv}\sigma_G^{g^{-dv}+u}=(\tau_G^v\sigma_G^{u+g^{-dv}})^\gamma$$

and

$$\tau^d\cdot(\tau_G^v\sigma_G^u)^\gamma=\tau_G^{dv+d}\sigma_G^u=(\tau_G^{v+1}\sigma_G^u)^\gamma.$$

Thus, dropping the subscripts G so that σ, τ are now generators of $G\cong C$ as in (3.4), we obtain the groups N_d described in the statement of the lemma. □

5.3. $m = q$

Lemma 5.2. *We have*

$$e(M,M,q) = p(q-2), \quad e(C,M,q) = q-1. \tag{5.6}$$

The $p(q-2)$ *subgroups of* $\mathrm{Perm}(M)$ *giving rise to the Hopf–Galois structures counted by* $e(M,M,q)$ *are the groups* $N_{a,b}$ *for* $1 \leqslant a \leqslant q-2$ *and* $0 \leqslant b \leqslant p-1$, *where* $N_{a,b}$ *is generated by the two permutations*

$$\sigma^u\tau^v \mapsto \sigma^{u+1}\tau^v, \quad \sigma^u\tau^v \mapsto \sigma^{g^a u + b(g^a s(v) - s(v-1))}\tau^{v-1}. \tag{5.7}$$

Here $\sigma^u\tau^v$ *denotes an arbitrary element of* M, *and* $s(v)$ *is defined in* (3.1), *with* $s(-1)$ *to be interpreted as* $s(q-1)$.

The $q-1$ *subgroups of* $\mathrm{Perm}(C)$ *giving rise to the Hopf–Galois structures counted by* $e(C,M,q)$ *are the groups* N'_d *for* $1 \leqslant d \leqslant q-1$, *where* N'_d *is generated by the two permutations*

$$\sigma^u\tau^v \mapsto \sigma^{u+1}\tau^v, \quad \sigma^u\tau^v \mapsto \sigma^{ug^d}\tau^{v-1}, \tag{5.8}$$

where now $\sigma^u\tau^v$ *denotes an arbitrary element of* C.

Proof. If G is a regular subgroup of $\mathrm{Hol}(M)$ with image of order q in $\mathrm{Aut}(M)$ then this image is generated by some $\theta = \alpha^b\beta$ with $0 \leqslant b \leqslant p-1$, where α and β are as in (3.7). Also, $G \cap M$ is the unique subgroup of M of order p. Thus

$$G = \langle \sigma, \tau^a\theta \rangle \tag{5.9}$$

with $1 \leqslant a \leqslant q-1$, where σ, τ are the generators of M as in (3.6). We determine when the group G defined by (5.9) has the required properties. Firstly we calculate

$$(\tau^a\theta)\sigma = \tau^a\sigma^\theta\theta = \tau^a\sigma^g\theta = \sigma^{g^{a+1}}(\tau^a\theta), \tag{5.10}$$

so the two generators commute if and only if $a = q-1$. It is easily seen that $(\tau^a\theta)^k$ has the form $\sigma^m\tau^{ka}\alpha^{bs(k)}\beta^k$ for some integer m (depending on a, b and k), so that $(\tau^a\theta)^q$ is a power of σ. Thus G has order pq, and in fact $(\tau^a\theta)^q = 1$ except possibly when $a = q-1$. The resulting groups are all distinct, and are regular on M. We therefore have $e'(M,M,q) = p(q-2)$ and $e'(C,M,q) = p$, giving (5.6).

We next determine the $q-1$ subgroups of $\mathrm{Perm}(C)$ counted by $e(C,M,q)$. We have $a = q-1$, and we may assume $b = 0$. Let $\sigma_G = \sigma$, $\tau_G = \tau^{-1}\beta$ be the generators of $G \cong C$ in (5.9). Then $\tau_G^v = \tau^{-v}\beta^v$, so for any $g = \sigma_G^u\tau_G^v \in G$ we have $\Phi(g) = \sigma^u\tau^{-v}$. Thus

$$\sigma \cdot g = \Phi^{-1}(\sigma^{u+1}\tau^{-v}) = \sigma_G^{u+1}\tau_G^v$$

and

$$\tau \cdot g = \Phi^{-1}(\tau\sigma^u\tau^{-v}) = \Phi^{-1}(\sigma^{gu}\tau^{1-v}) = \sigma_G^{gu}\tau_G^{v-1}.$$

We conjugate this action by the $q-1$ automorphisms γ of C defined in (5.5): this yields

$$\sigma \cdot (\sigma_G^u\tau_G^v)^\gamma = (\sigma_G^{u+1}\tau_G^v)^\gamma$$

and

$$\tau^d \cdot (\sigma_G^u \tau_G^v)^\gamma = \Phi^{-1}(\tau^d \sigma^u \tau^{-vd}) = \sigma_G^{ug^d} \tau_G^{dv-d} = (\sigma_G^{ug^d} \tau_G^{v-1})^\gamma,$$

giving the $q-1$ groups N'_d defined by (5.8).

To describe the $p(q-2)$ subgroups M of $\mathrm{Perm}(M)$ counted by $e(M,M,q)$, we must still examine the action of M on G given by (2.2), even though in this case G and M are isomorphic. Note however that we cannot identify the generator $\tau^a\theta$ of G in (5.9) with the generator τ of M, since the commutation relations (3.6) and (5.10) are not compatible. To simplify our calculations, we shall first identify the $q-2$ actions of M on itself corresponding to the case $b=0$. We shall then conjugate by suitable automorphisms of M in order to obtain the actions corresponding to the other values of b.

Taking $b=0$, we have $(\tau^a\theta)^k = (\tau^a\beta)^k = \tau^{ak}\beta^k$ for all k. Let h satisfy $(a+1)h \equiv 1 \pmod q$, so that as a runs through $1 \leqslant a \leqslant q-2$, we may take h to run through $2 \leqslant h \leqslant q-1$. Then G is generated by $\sigma_G = \sigma$ and $\tau_G = (\tau^a\theta)^h = \tau^{1-h}\beta^h$, and we have the same commutation relation $\tau_G\sigma_G = \sigma_G^g\tau_G$ as in (3.6). We calculate

$$\Phi(\sigma_G^u \tau_G^v) = \sigma^u \tau^{v(1-h)}.$$

To simplify notation, redefine a by $a = h-1$. Then

$$\Phi(\sigma_G^u \tau_G^v) = \sigma^u \tau^{-va},$$

so that

$$\sigma \cdot \sigma_G^u \tau_G^v = \sigma_G^{u+1} \tau_G^v$$

and

$$\tau^a \cdot \sigma_G^u \tau_G^v = \sigma_G^{g^a u} \tau_G^{v-1}.$$

Letting $1 \leqslant a \leqslant q-2$, this gives the $q-2$ subgroups $N \cong M$ of $\mathrm{Perm}(G)$ for $b=0$. We now conjugate by the automorphisms $\gamma = \alpha^b$ of $G \cong M$, where $0 \leqslant b \leqslant p-1$ and α is as defined in (3.7). We calculate

$$\sigma \cdot (\sigma_G^u \tau_G^v)^\gamma = \sigma_G^{1+u} (\sigma_G^b \tau_G)^v = (\sigma_G^{u+1} \tau_G^v)^\gamma$$

and

$$\tau^a \cdot (\sigma_G^u \tau_G^v)^\gamma = \Phi^{-1}(\tau^a \sigma^{u+bs(v)} \tau^{-va}) = (\sigma_G^{u'} \tau_G^{v-1})^\gamma,$$

where $u' + bs(v-1) = g^a(u + bs(v))$. This gives the groups $N_{a,b}$ of (5.7). □

5.4. $m = pq$

We begin by determining the effect of $\sigma^{a_0}\alpha \in \mathrm{Hol}(M)$, where a_0 is defined in (3.3) and $\alpha \in \mathrm{Aut}(M)$ is defined in (3.7).

Proposition 5.3. *$\sigma^{a_0}\alpha$ acts on M as right multiplication by σ^{a_0}.*

Proof. For an arbitrary element $g=\sigma^u\tau^v$ of M we have

$$(\sigma^{a_0}\alpha)\cdot g=\sigma^{a_0+u}(\sigma\tau)^v=\sigma^{a_0+u+s(v)}\tau^v$$

and

$$g\sigma^{a_0}=\sigma^{u+a_0g^v}\tau^v,$$

so we must verify the congruence

$$a_0+u+s(v)\equiv u+a_0g^v \pmod p.$$

Multiplying by $g-1$ and using (3.3), this is equivalent to $1+(g-1)s(v)\equiv g^v \pmod p$, which is immediate from (3.1). □

We can now treat the final case.

Lemma 5.4. *We have*

$$e(M,M,pq)=p(q-2)+1, \quad e(C,M,pq)=0. \tag{5.11}$$

The $p(q-2)+1$ *subgroups of* $\mathrm{Perm}(M)$ *giving rise to the corresponding Hopf–Galois structures are the group of right translations by* M (*which gives the classical Hopf–Galois structure*) *and the groups* $N_{c,d}$ *for* $0\leqslant c\leqslant p-1$ *and* $1\leqslant d\leqslant q-2$, *where* $N_{c,d}$ *is generated by the two permutations*

$$\sigma^u\tau^v\mapsto\sigma^{u+g^{-vd}}\tau^v, \quad \sigma^u\tau^v\mapsto\sigma^{u+cg^{-vd}(s(v,d+1)-g^{-d}s(v+1,d+1))}\tau^{v+1}. \tag{5.12}$$

Here $\sigma^u\tau^v$ *denotes an arbitrary element of* M, *and* $s(r,d)$ *is defined in* (3.2).

Proof. Any regular subgroup G of $\mathrm{Hol}(M)$ which surjects onto $A(M)\subset\mathrm{Aut}(M)$ must be isomorphic to M, so $e(C,M,pq)=0$. Moreover, G must have the form

$$G=\langle\eta\alpha,\nu\beta\rangle \tag{5.13}$$

for some elements $\eta=\sigma^a\tau^b$ and $\nu=\sigma^c\tau^d$ of M. Here σ, τ are as in (3.6), α, β as in (5.7), and we can assume that $0\leqslant a,c\leqslant p-1$ and $0\leqslant b,d\leqslant q-1$. Conversely, given η, $\nu\in M$, the group G defined by (5.13) will have order pq if and only if $\eta\alpha$ and $\nu\beta$ satisfy the same relations as the generators α, β of $A(M)$, and G will be regular on M if and only if furthermore G acts transitively on M.

We first determine when $\eta\alpha$ has order p. We have

$$\eta^\alpha=\sigma^a(\sigma\tau)^b=\sigma^{a+s(b)}\tau^b$$

and inductively,

$$\eta^{\alpha^k}=\sigma^{a+ks(b)}\tau^b.$$

Thus

$$(\eta\alpha)^p=\eta^{1+\alpha+\cdots+\alpha^{p-1}}\alpha^p=(\sigma^a\tau^b)(\sigma^{a+s(b)}\tau^b)\ldots(\sigma^{a+(p-1)s(b)}\tau^b)=\sigma^m\tau^{pb}$$

for some m. If $\eta\alpha$ has order p we must have $b=0$, and conversely if $b=0$ then $(\eta\alpha)^p=\sigma^{ap}=1$. Thus we are reduced to considering

$$G=\langle\sigma^a\alpha,\nu\beta\rangle,$$

the first generator having order p. If this group has order pq, it will be regular on M provided that $d \neq 0$.

Next consider the relation

$$(v\beta)(\sigma^a\alpha) = (\sigma^a\alpha)^g(v\beta). \tag{5.14}$$

As $\sigma^\alpha = \sigma$ and $\sigma^\beta = \sigma^g$, this simplifies to $v\sigma^{ag}\beta\alpha = \sigma^{ag}v^{\alpha^g}\alpha^g\beta$. Thus (5.14) holds if and only if $v\sigma^{ag} = \sigma^{ag}v^{\alpha^g}$.

Now $(\tau^d)^{\alpha^q} = (\sigma^g\tau)^d = \sigma^{gs(d)}\tau^d$. Thus $v^{\alpha^g} = \sigma^{c+gs(d)}\tau^d$, and (5.14) is equivalent to $\sigma^{c+ag^{d+1}}\tau^d = \sigma^{ag+c+gs(d)}\tau^d$, and hence to $ag^{d+1} \equiv ag + gs(d) \pmod p$. This may be written $a(g^d - 1) \equiv s(d) \pmod p$. Using (3.1) and (3.3), we conclude that (5.14) holds if and only if $a = a_0$. Thus by Proposition 5.3, G contains right multiplication by σ.

Finally we require $v\beta$ to have order q. Now $v^{\beta^r} = \sigma^{cg^r}\tau^d$, so

$$\begin{aligned}(v\beta)^v &= v^{1+\beta+\cdots+\beta^{v-1}}\beta^v \\ &= (\sigma^c\tau^d)(\sigma^{cg}\tau^d)\ldots(\sigma^{cg^{v-1}}\tau^d)\beta^v \\ &= \sigma^{cs(v,d+1)}\tau^{vd}\beta^v. \end{aligned} \tag{5.15}$$

Take $v = q$. If $d \neq q-1$ then by (3.2) we have $s(q, d+1) \equiv 0 \pmod p$, so $(v\beta)^q = 1$ for any choice of c. If $d = q-1$ then $s(q, d+1) = s(q,q) \equiv q \not\equiv 0 \pmod p$ and we must take $c = 0$. We have now shown that G in (5.13) is isomorphic under Θ to $A(M)$ precisely for $\eta = \sigma^{a_0}$, $v = \sigma^c\tau^d$ with either $d \neq q-1$ or $c = 0$. Moreover, G will then be regular on M except when $d = 0$. This gives $e'(M, M, pq) = p(q-2)+1$, completing the proof of (5.11).

We now describe the corresponding subgroups N of $\mathrm{Perm}(M)$. In the exceptional case $c = 0$, $d = q-1$ we have

$$(v\beta)\cdot(\sigma^u\tau^v) = (\tau^{-1}\beta)\cdot(\sigma^u\tau^v) = \tau^{-1}\sigma^{gu}\tau^v = \sigma^u\tau^{v-1}.$$

Thus G is the group of right translations by M, corresponding to the classical Hopf–Galois structure on the field extension L/K. In the remaining cases $0 \leqslant c \leqslant p-1$, $1 \leqslant d \leqslant q-2$, we write $\sigma_G = \sigma^{a_0}\alpha$ and $\tau_G = v\beta$ for the generators of G in (5.13). From (5.15) and Proposition 5.3, we have

$$\Phi(\sigma_G^u\tau_G^v) = \tau_G\cdot\sigma^u = \sigma^{cs(v,d+1)+ug^{vd}}\tau^{vd}.$$

Hence

$$\sigma\cdot\sigma_G^u\tau_G^v = \sigma_G^{u+g^{-vd}}\tau_G^v$$

and

$$\tau^d\cdot\sigma_G^u\tau_G^v = \Phi^{-1}(\sigma^{g^d(cs(v,d+1)+ug^{vd})}\tau^{(v+1)d}) = \sigma_G^{u'}\tau_G^{v+1},$$

where

$$cs(v+1, d+1) + u'g^{(v+1)d} = g^d(cs(v,d+1) + ug^{vd}),$$

that is,

$$u' = u + cg^{-(v+1)d}(g^d s(v,d+1) - s(v+1,d+1)).$$

We therefore obtain the $p(q-2)$ groups $N_{c,d}$ described in (5.12). □

6. Counting the Hopf–Galois structures

Adding up the contributions from (4.1), (4.2), (5.1), (5.2), (5.6) and (5.11), we find that $e(C,C)=1$, $e(C,M)=2(q-1)$ and $e(M,M)=2+2p(q-2)$, $e(M,C)=p$. We may therefore summarise the preceding calculations in the following two results.

Theorem 6.1. *Let L/K be a cyclic extension of fields of degree pq, where p, q are primes with $p\equiv 1 \pmod q$. Then L/K admits precisely $2q-1$ Hopf–Galois structures. Only the classical Hopf–Galois structure is of cyclic type. The other $2(q-1)$ Hopf–Galois structures are of nonabelian type. The corresponding subgroups of* $\mathrm{Perm}(C)$ *are the $q-1$ groups generated by the permutations* (5.3) *for $1\leqslant d\leqslant q-1$, and the $q-1$ groups generated by the permutations* (5.8) *for $1\leqslant d\leqslant q-1$.*

Theorem 6.2. *Let L/K be a nonabelian Galois extension of fields of degree pq, where p, q are primes with $p\equiv 1 \pmod q$. Then L/K admits precisely $2+p(2q-3)$ Hopf–Galois structures, of which $2+2p(q-2)$ are of nonabelian type and the remaining p are of cyclic type. The subgroups of* $\mathrm{Perm}(M)$ *giving the Hopf–Galois structures of nonabelian type are the group of left translations by M, the group of right translations by M (which gives the classical Hopf–Galois structure), the $p(q-2)$ groups generated by the permutations* (5.7) *for $1\leqslant a\leqslant q-2$, $0\leqslant b\leqslant p-1$, and the $p(q-2)$ groups generated by the permutations* (5.12) *for $0\leqslant c\leqslant p-1$, $1\leqslant d\leqslant q-2$. The subgroups of* $\mathrm{Perm}(M)$ *giving the Hopf–Galois structures of cyclic type are the p groups generated by the permutations in* (4.3) *for $0\leqslant c\leqslant p-1$.*

Remark 6.3. One can easily extract from the proofs of Lemmas 4.1, 5.1, 5.2 and 5.4 the relations satisfied by the two permutations generating each of the groups N. In each case, denote the two given generators by S, T, respectively. In all cases we have $S^p=1=T^q$. In (4.3), we have $N\cong C$ so of course $TS=ST$. In the two cases where $G\cong N\cong M$, namely (5.7) and (5.12), we have $TS=S^{g^a}T$ and $TS=S^{g^d}T$, respectively. In (5.3) and (5.8), where $G\cong C$ and $N\cong M$, we again have $TS=S^{g^d}T$.

We end with some examples.

Corollary 6.4. *For any odd prime p, a cyclic extension of degree $2p$ has 3 Hopf–Galois structures, namely the classical one and 2 of dihedral type.*

Corollary 6.5. *For an odd prime p, a dihedral extension of degree $2p$ has 2 Hopf–Galois structures of dihedral type and p Hopf–Galois structures of cyclic type. In particular, an extension with Galois group S_3 (the symmetric group on 3 letters) has in total 5 Hopf–Galois structures, of which 2 have type S_3 and 3 have cyclic type.*

Corollary 6.6. *Let L/K be a Galois extension of degree 21. If it is cyclic, it has 5 Hopf–Galois structures, of which all but the classical one are of nonabelian type. If the extension is nonabelian, it has 23 Hopf–Galois structures, of which 7 have cyclic type and 16 have nonabelian type.*

References

[1] N.P. Byott, Uniqueness of Hopf–Galois structure for separable field extensions, Comm. Algebra 24 (1996) 3217–3228, Corrigendum, 3705.
[2] N.P. Byott, Hopf–Galois structures on field extensions with simple Galois groups, Bull. London Math. Soc., to appear.
[3] S. Carnahan, L. Childs, Counting Hopf–Galois structures on non-abelian Galois field extensions, J. Algebra 218 (1999) 81–92.
[4] L.N. Childs, On the Hopf–Galois theory for separable field extensions, Comm. Algebra 17 (1989) 809–825.
[5] L.N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, Mathematical Surveys and Monographs, Vol. 80, American Mathematical Society, Providence RI, 2000.
[6] L.N. Childs, On Hopf–Galois structures and complete groups, New York J. Math 9 (2003) 99–115.
[7] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987) 239–258.
[8] T. Kohl, Classification of the Hopf Galois structures on prime power radical extensions, J. Algebra 207 (1998) 525–546.